

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200314975-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Bruce Edward LAVIGNE et al.

Confirmation No.: 5129

Application No.: 10/813,730

Examiner: Devin E. ALMEIDA

Filing Date: March 31, 2004

Group Art Unit: 2432

Title: SECURE REMOTE MIRRORING

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 3, 2009.

☒ The fee for filing this Appeal Brief is \$540.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month
\$130

☐ 2nd Month
\$490

☐ 3rd Month
\$1110

☐ 4th Month
\$1730

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 540. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Bruce Edward LAVIGNE et al.

By:


Asbok K. Mannava

Attorney/Agent for Applicant(s)

Reg No. : 45,301

Date : November 3, 2009

Telephone : (703) 652-3822

PATENT

Atty Docket No.: 200314975-1
App. Ser. No.: 10/813,730

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Bruce Edward LAVIGNE et al.	Confirmation No.:	5129
Serial No.:	10/813,730	Examiner:	Devin E. ALMEIDA
Filed:	March 31, 2004	Group Art Unit:	2432
Title:	SECURE REMOTE MIRRORING		

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action mailed August 3, 2009, and in connection with the Notice of Appeal filed herewith.

It is respectfully submitted that the present application has been at least twice rejected.

Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

TABLE OF CONTENTS

(1)	Real Party in Interest.....	3
(2)	Related Appeals And Interferences.....	3
(3)	Status of Claims.....	3
(4)	Status of Amendments	3
(5)	Summary of Claimed Subject Matter	3
(6)	Grounds of Rejection to be Reviewed on Appeal.....	9
(7)	Arguments	10
	A. The rejection of claims 1, 4, 7-10, 14 and 16-23 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada and Amara should be reversed.....	10
	B. The rejection of claims 5 and 6 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada and Kojima should be reversed.	14
	C. The rejection of claim 12 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada, Amara, and Classon should be reversed.	15
	D. The rejection of claim 13 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Amara and Engwer should be reversed.	16
(8)	Conclusion	17
(9)	Claim Appendix	18
(10)	Evidence Appendix	26
(11)	Related Proceedings Appendix	27

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3) Status of Claims

Claims 1, 4-14 and 16-23 are pending in the present application and stand rejected.

Claims 2, 3, and 15 have been canceled.

Pursuant to 37 C.F.R. § 41.37, the Appellants hereby appeal the Examiner's decision finally rejecting all of the pending claims to the Board of Patent Appeals and Interferences. Therefore, claims 1, 4-14 and 16-23 of this application are appealed.

(4) Status of Amendments

No amendment was filed subsequent to the Final Office Action dated August 3, 2009.

A copy of the claims at issue on appeal is attached hereto as the Claims Appendix.

(5) Summary of Claimed Subject Matter

Claims 1, 14, 17, 20 and 21 are the independent claims in this appeal. It should be understood that the citations below to the original disclosure as providing support for the claimed features are merely exemplary and do not limit the claim features to only those citations.

Claim 1. A method (Fig. 2) for secure remote mirroring of network traffic, the method comprising:

receiving a data packet to be remotely mirrored by an entry device (entry device 102 in Fig. 1) pre-configured with a mirroring destination address to which to mirror the data packet (step 204 in Fig. 2; *Specification*, page 6, lines 28-29);

forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet (step 308 in Fig. 3; page 9, lines 1-2);

encrypting a copy of the data packet to form an encrypted packet (step 206 in Fig. 2; page 6, lines 31-33);

incrementing an identifier to indicate a position of the encrypted packet within an order of packets received by an exit device (page 8, lines 6-7);

generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address and said identifier, the second header includes a media access control (MAC) destination address, and the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet including the IP destination address (steps 208 and 210 in Fig. 2; headers 434 and 432 in Fig. 4D; “identifier” on page 8, lines 6-7); and

forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address (step 212 in Fig. 2; page 7, lines 11-12).

Claim 14. A networking device (switch 500 in Fig. 5) comprising:

a plurality of ports (504 in Fig. 5) for receiving and transmitting packets therefrom, wherein the packets are transmitted based on original destination addresses indicated therein (page 9, lines 28-31);

a secure remote mirroring engine (510 in Fig. 5) configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets, to encrypt copies of the detected packets, to encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes said identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) destination address, and to forward the encapsulated encrypted packets to a pre-configured destination address corresponding to the IP destination address by way of at least one of the ports (*Specification*, page 10, lines 9-15; “identifier” on page 8, lines 6-7); and
an encryption module (512 in Fig. 5) configured to be utilized by the remote mirroring engine during encryption of the detected packets (page 10, lines 15-16).

Claim 17. A system (Figs. 1, 5, and 6) for secure remote mirroring of network traffic, the system comprising:

a mirror entry device (102 in Fig. 1; 500 in Fig. 5) including a secure mirroring engine (510) configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets from the specified mirror source, to encrypt copies of the detected packets using an encryption module, encapsulate each of the encrypted

packets by adding, to the encrypted packet, a first header which includes said identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) destination address, and to forward the encapsulated encrypted packets to a pre-configured destination corresponding to the IP destination address by way of at least one of the ports, wherein the pre-configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations (page 10, lines 9-15; “identifier” on page 8, lines 6-7); and

a mirror exit device (108 in Fig. 1; 600 in Fig. 6) including a secure mirroring receiver (610 in Fig. 6) configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets (from page 8, line 31 to page 9, line 6).

Claim 20. A system (Fig. 1) for secure remote mirroring of network traffic, the system comprising:

a mirror entry device (102 in Fig. 1; 500 in Fig. 5) including means to encrypt copies of the detected packets using an encryption module and to encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes an incrementing identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) address, wherein the IP destination address corresponds to a pre-configured destination address of a mirror exit device and the pre-

configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations (page 10, lines 9-16; and page 8, lines 6-7); and

the mirror exit device (108 in Fig. 1; 600 in Fig. 6) including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets (from page 8, line 31 to page 9, line 6).

Claim 21. A method (Fig. 2) for secure remote mirroring of network traffic, the method comprising:

remotely configuring an entry device (102 in Fig. 1) with an encryption key and mirroring destination address (page 6, lines 21-22);

remotely configuring an exit device (108 in Fig. 1) at the mirroring destination address with a decryption key (page 8, lines 19-20);

receiving a data packet to be mirrored by the entry device (204 in Fig. 2);

incrementing an identifier to indicate a position of the data packet within an order of packets mirrored by the entry device (page 8, lines 6-7);

encrypting a copy of the data packet using the encryption key to form an encrypted packet (206 in Fig. 2; page 6, lines 31-33);

generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address and said identifier and the

second header includes a media access control (MAC) destination address (208 in Fig. 2; page 8, lines 6-7; and page 7, lines 10-32);

forwarding the data packet in unencrypted form to an original destination address indicated in the data packet (308 in Fig. 3; page 9, lines 1-2); and

forwarding the encapsulated encrypted packet to the mirroring destination address of the exit device (212 in Fig. 2; page 7, lines 11-12).

(6) Grounds of Rejection to be Reviewed on Appeal

A. Whether claims 1, 4, 7-10, 14 and 16-23 were properly rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0213232 to Regan (hereinafter “Regan”) in view of U.S. Patent No. 6,775,769 to Inada et al. (hereinafter “Inada”) and in further view of U.S. Patent No. 6,839,338 to Amara et al. (hereinafter “Amara”).

B. Whether claims 5 and 6 were properly rejected under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada and in further view of U.S. Patent No. 5,280,476 to Kojima et al. (hereinafter “Kojima”).

C. Whether claim 12 was properly rejected under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada, Amara, and U.S. Patent No. 6,700,867 to Classon et al. (hereinafter “Classon”).

D. Whether claim 13 was properly rejected under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Amara and U.S. Patent No. 6,947,483 to Engwer (hereinafter “Engwer”).

(7) Arguments

A. The rejection of claims 1, 4, 7-10, 14 and 16-23 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada and Amara should be reversed.

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007):

“Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.” Quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966).

According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of *KSR International Co. v. Teleflex Inc.*, Federal Register, Vol. 72, No. 195, 57526, 57529 (October 10, 2007), once the *Graham* factual inquiries are resolved, there must be a determination of whether the claimed invention would have been obvious to one of ordinary skill in the art based on any one of the following proper rationales:

(A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) “Obvious to try”—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G)

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in *KSR International Co. v. Teleflex Inc.*, quoting from *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006), “[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness.”

Furthermore, as set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, “[a]ll claim limitations must be considered” because “all words in a claim must be considered in judging the patentability of that claim against the prior art.” *In re Wilson*, 424 F.2d 1382, 1385.

- **Claims 1, 4, 7-10, 14, and 16-23**

Claims 1, 4, 7-10, 14, and 16-23 were rejected 35 U.S.C. §102(e), as being anticipated by Regan in view of Inada and further in view of Amara. This rejection should be reversed for at least the following reasons.

- **Independent Claim 1:**

Claim 1 recites, among other elements, “the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address **and said identifier**” wherein the “identifier” is “to indicate a position of the encrypted packet within an order of

packets received by an exit device.” The combination of Regan, Inada and Amara fails to teach or suggest at least the claimed “first header” having an IP destination address and an identifier, as recited in claim 1 for at least the following reasons.

In the Final Office Action, the Examiner correctly admits that Regan does not teach or suggest a first header including an IP destination address and an identifier, as recited in claim 1 (See *Final Office Action*, page 4). The Examiner then relies upon Inada for teaching that first header. More specifically, the Examiner asserts that the “new IP header” disclosed in col. 11, lines 43-52 of Inada is the “first header” recited in claim 1 (See *Final Office Action*, page 4 and “Response to Arguments” on page 2). However, that assertion is respectfully traversed because col. 11, lines 43-52 of Inada discloses a new IP header having an IP address. As such, the passage in col. 11, lines 43-52 of Inada **does not mention or suggest that the new IP header also includes the identifier of claim 1, in addition to the IP address**. In fact, nowhere in Inada teaches or suggest a packet having a header that includes both an IP destination address and an identifier, let alone the specific identifier described in claim 1. Therefore, Inada fails to teach or suggest the “first header” including an IP destination address and the identifier indicating a position of the encrypted packet within an order of packets received by an exit device, as recited in claim 1. As a result, Inada fails to cure the deficiencies of Regan.

Amara also fails to teach or suggest a header including an IP destination address and the identifier recited in claim 1. Although Amara discloses in Fig. 4 an IP header having a sequence number field 210, the IP header of Amara does not have both an IP destination address and an identifier that indicates the position of encrypted packets within the order of packets received by

an exit device, as recited in claim 1. Therefore, Amara fails to cure the deficiencies of Regan and Inada.

At least for the reasons set forth above, the proposed combination of Regan, Inada and Amara fails to establish a *prima facie* case of obviousness against independent claim 1. Therefore, it is respectfully requested that the rejection of independent claim 1 be reversed, and this claim be allowed.

- Independent Claims 14, 17, 20 and 21:

Independent claims 14, 17, 20 and 21 each recite a first header including an IP destination address and an identifier, similar to claim 1. Thus, claims 14, 17, 20 and 21 are also believed to be allowable over the combination of Regan, Inada and Amara for at least the same reasons set forth above with respect to claim 1. It is therefore respectfully requested that the rejection of independent claims 14, 17, 20 and 21 be reversed, and these claims be allowed.

- Dependent Claims 4, 7-10, 16, 18-19 and 22-23:

Claims 4, 7-10, 16, 18-19 and 22-23 are dependent from one of independent claim 1, 14, 17 and 21. Thus, they are also believed to be allowable over the cited documents of record for at least the same reasons set forth above. It is therefore respectfully requested that the rejection of claims 4, 7-10, 16, 18-19 and 22-23 be reversed, and these claims be allowed.

B. The rejection of claims 5 and 6 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada and Kojima should be reversed.

Claims 5 and 6 were rejected under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada and Kojima. This rejection is respectfully traversed for at least as follows.

Claims 5 and 6 are dependent from independent claim 1. As discussed above, the proposed combination of Regan and Inada fails to disclose all of the features of independent claim 1. In setting forth the rejection of claims 5 and 6, the Final Office Action has not and cannot reasonably assert that the disclosure contained in Kojima makes up for any of the deficiencies discussed above with respect to the proposed combination. Accordingly, even assuming for the sake of argument that one of ordinary skill in the art were somehow motivated to modify the proposed combination of Regan and Inada with the disclosure contained in Kojima, the proposed modification would still fail to yield all of the features of independent claim 1, from which claims 5 and 6 depend.

In addition, independent claim 1 was rejected under Regan in view of Inada and further in view of Amara. Claims 5 and 6 depend from independent claim 1. However, the rejection of claims 5 and 6 fails to include Amara, which was used in the rejection of independent claim 1 as allegedly teaching “incrementing an identifier to indicate a position of the encrypted packet within an order of packets received by an exit device,” to overcome the deficiencies of Regan. Kojima fails to teach such “incrementing” feature. The rejection of claims 5 and 6 also fails to point out a teaching of that “incrementing” feature in Kojima. Therefore, Kojima fails to cure at

least that deficiency of Regan, and the rejection of claims 5 and 6 based on Regan, Inada and Kojima should be reversed.

C. The rejection of claim 12 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Inada, Amara, and Classon should be reversed.

Claim 12 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Regan in view of Inada, Amara and Classon. This rejection is respectfully traversed for at least the following reasons.

Claim 12 is dependent from independent claim 1. As discussed above, the proposed combination of Regan, Inada and Amara fails to disclose all of the features of independent claim 1. In setting forth the rejection of claim 12, the Final Office Action has not and cannot reasonably assert that the disclosure contained in Classon makes up for any of the deficiencies discussed above with respect to the proposed combination. Accordingly, even assuming for the sake of argument that one of ordinary skill in the art were somehow motivated to modify the proposed combination of Regan, Inada and Amara with the disclosure contained in Classon, the proposed modification would still fail to yield all of the features of independent claim 1, from which claim 12 depends.

For at least the foregoing reasons, the Final Office Action has failed to establish that claim 12 is *prima facie* obvious in view of the combined disclosures contained in Regan, Inada, Amara and Classon, as proposed in the Final Office Action. It is therefore respectfully requested that the rejection of claim 12 be reversed, and this claim be allowed.

D. The rejection of claim 13 under 35 U.S.C. §103(a) as being unpatentable over Regan in view of Amara and Engwer should be reversed.

Claim 13 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Regan in view of Amara and Engwer. This rejection is respectfully traversed for at least the following reasons.

Claim 13 is dependent from independent claim 1. As discussed above, the proposed combination of Regan and Amara fails to disclose all of the features of independent claim 1. In setting forth the rejection of claim 13, the Office Action has not and cannot reasonably assert that the disclosure contained in Engwer makes up for any of the deficiencies discussed above with respect to the proposed combination. Accordingly, even assuming for the sake of argument that one of ordinary skill in the art were somehow motivated to modify the proposed combination of Regan and Amara with the disclosure contained in Engwer, the proposed modification would still fail to yield all of the features of independent claim 1, from which claim 13 depends.

In addition, the rejection of claim 13 fails to include Inada, which was used in the rejection of claim 1 as allegedly teaching the first header that includes the IP destination and the identifier, to overcome the deficiencies of Regan. Engwer fails to teach such a first header. The Final Office Action also fails to point out a teaching of such a first header in Engwer. Therefore, Engwer fails to at least cure the deficiencies in Regan.

For at least the foregoing reasons, the Final Office Action has failed to establish that claim 13 is *prima facie* obvious in view of the combined disclosures contained in Regan, Amara

PATENT

Atty Docket No.: 200314975-1
App. Ser. No.: 10/813,730

and Engwer, as proposed in the Final Office Action. It is therefore respectfully requested that the rejection of claim 13 be reversed, and this claim be allowed.

(8) Conclusion

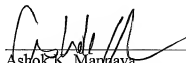
For at least the reasons given above, the rejection of claims 1, 4-14 and 16-23 described above should be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: November 3, 2009

By


Ashok K. Manjava
Registration No.: 45,301
(703) 652-3822

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 865-5150 (facsimile)

(9) Claim Appendix

1. (Previously Presented) A method for secure remote mirroring of network traffic, the method comprising:

receiving a data packet to be remotely mirrored by an entry device pre-configured with a mirroring destination address to which to mirror the data packet;

forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet;

encrypting a copy of the data packet to form an encrypted packet;

incrementing an identifier to indicate a position of the encrypted packet within an order of packets received by an exit device;

generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address and said identifier, the second header includes a media access control (MAC) destination address, and the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet including the IP destination address; and

forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address.

2 and 3. (Canceled)

4. (Previously Presented) The method of claim 1, further comprising:
determining the MAC destination address associated with the IP destination address;
generating and adding, as the second header, a MAC header including the MAC destination address to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC destination address in a destination field; and
transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain.
5. (Previously Presented) The method of claim 4, wherein determining the MAC destination address comprises:
determining if a mapping of the IP destination address to the MAC destination address is stored in an address resolution protocol (ARP) cache;
if so, then retrieving the MAC destination address from the ARP cache; and
if not, then broadcasting an ARP request with the IP destination address and receiving an ARP reply with the MAC destination address.
6. (Previously Presented) The method of claim 4, wherein the IP-encapsulated encrypted packet is communicated across multiple intermediate layer 2 domains.

7. (Previously Presented) The method of claim 1, further comprising:
receiving the encapsulated encrypted packet by the exit device;
removing the headers to de-encapsulate the encrypted packet; and
decrypting the encrypted packet to re-generate the data packet; and
using said identifier to determine the position of the data packet within the order of
packets received by the exit device.
8. (Original) The method of claim 7, wherein the encrypting and decrypting is performed
under a public-private key encryption scheme.
9. (Original) The method of claim 8, wherein the encrypting is performed using a public key
of a destination device, and wherein the decrypting is performed using a corresponding private
key of the destination device.
10. (Original) The method of claim 1, further comprising:
configuring the entry device in a best effort mirroring mode to reduce head-of-line
blocking.
11. (Original) The method of claim 1, further comprising:
configuring the entry device in a lossless mirroring mode to assure completeness of
mirrored traffic.

12. (Original) The method of claim 1, further comprising:
truncating the data packet to reduce a size of the data packet prior to encryption thereof.
13. (Original) The method of claim 1, further comprising:
compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption thereof.
14. (Previously Presented) A networking device comprising:
a plurality of ports for receiving and transmitting packets therefrom, wherein the packets are transmitted based on original destination addresses indicated therein;
a secure remote mirroring engine configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets, to encrypt copies of the detected packets, to encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes said identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) destination address, and to forward the encapsulated encrypted packets to a pre-configured destination address corresponding to the IP destination address by way of at least one of the ports; and
an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

15. (Canceled)

16. (Previously Presented) The networking device of claim 14, wherein the remote mirroring engine encrypts the copies of the detected packets using a public key of a public-private key pair.

17. (Previously Presented) A system for secure remote mirroring of network traffic, the system comprising:

a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets from the specified mirror source, to encrypt copies of the detected packets using an encryption module, encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes said identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) destination address, and to forward the encapsulated encrypted packets to a pre-configured destination corresponding to the IP destination address by way of at least one of the ports, wherein the pre-configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations; and

a mirror exit device including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.

18. (Original) The system of claim 17, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

19. (Original) The system of claim 18, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.

20. (Previously Presented) A system for secure remote mirroring of network traffic, the system comprising:

a mirror entry device including means to encrypt copies of the detected packets using an encryption module and to encapsulate each of the encrypted packets by adding, to the encrypted packet, a first header which includes an incrementing identifier and an Internet Protocol (IP) destination address and by also adding a second header which includes a media access control (MAC) address, wherein the IP destination address corresponds to a pre-configured destination address of a mirror exit device and the pre-configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations; and

the mirror exit device including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.

21. (Previously Presented) A method for secure remote mirroring of network traffic, the method comprising:

remotely configuring an entry device with an encryption key and mirroring destination address;

remotely configuring an exit device at the mirroring destination address with a decryption key;

receiving a data packet to be mirrored by the entry device;

incrementing an identifier to indicate a position of the data packet within an order of packets mirrored by the entry device;

encrypting a copy of the data packet using the encryption key to form an encrypted packet;

generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol (IP) destination address corresponding to the mirroring destination address and said identifier and the second header includes a media access control (MAC) destination address;

forwarding the data packet in unencrypted form to an original destination address indicated in the data packet; and

forwarding the encapsulated encrypted packet to the mirroring destination address of the exit device.

PATENT

Atty Docket No.: 200314975-1

App. Ser. No.: 10/813,730

22. (Original) The method of claim 21, wherein the remote configuration is performed by way of SNMP.

23. (Original) The method of claim 21, wherein the remote configuration is performed by way of a secure remote protocol.

PATENT

Atty Docket No.: 200314975-1

App. Ser. No.: 10/813,730

(10) Evidence Appendix

None.

PATENT

Atty Docket No.: 200314975-1

App. Ser. No.: 10/813,730

(11) Related Proceedings Appendix

None.